The Thesis Committee for Jerald Adam Webber
Certifies that this is the approved version of the following thesis:

An Engineering Manager's Perspective on System Safety

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor: _____
Robert B. McCann

Supervisor: _____
Anthony P. Ambler

_____
Steven C. Snell

An Engineering Manager's Perspective on System Safety

by

Jerald Adam Webber, B.S.

Thesis

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin

December 2010

Abstract

An Engineering Manager's Perspective on System Safety

Jerald Adam Webber, MSE

The University of Texas at Austin, 2010

Supervisors: Robert B. McCann and Anthony P. Ambler

The science of system safety provides a structured guideline for managers to follow in order to ensure safe operations, but it does not ensure against deviations from such guidelines. This responsibility lies with management. Engineering managers must be able to dictate and track safety requirements throughout product development, deployment, and operation by treating system safety as an integrated engineering discipline. It is not feasible to expect the technical teams to integrate safety into designs unless safety requirements are considered a design metric just as cost and performance. Therefore, the traditional method of employing a separate safety department to address safety requirements is not sufficient. This responsibility must be given to all technical departments and levied as a design requirement.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

One doesn't have to search for very long to gain an understanding of the importance of system safety. Take for instance the sinking of Titanic. System safety was compromised during the design phase when engineers were forced to use low grade steel as opposed to the industry standard of the time [1]. Safety was again compromised during operations, on the day of the sinking, when communication between the radio room and the bridge broke down, binoculars were not present in the crow's nest, and only 20 lifeboats were present on a ship that was designed to hold 32 [1]. The consequence of this accident was 1500 people dead and loss of a $400 million asset (in today's dollars).

The Exxon Valdez oil spill is another example of the importance of uncompromising system safety principles. As was the case with Titanic, system safety was bypassed during both the design and operations phases of the Exxon Valdez program. First, during the design phase it was decided that the ship would be designed with a single hull. At the time, it was common for oil carrying ships to have a double hull design to minimize the loss of oil and reduce the environmental impact in the event of an accident. Proper system safety principles would call for a double hull design as a risk mitigation measure to protect the integrity of the ship when exposed to the hazards present in the shipping lanes off the coast of Alaska. If management had given proper consideration to the consequences of an oil spill on the environment, it would have been clear that a double hull design was necessary. As far as operations go, at the time of the spill the shipmaster was sleeping off a hang-over while the Third Mate attempted to

maneuver the ship through the precarious shipping lane off the coast of Alaska. The shipmaster suffered from alcoholism and had been through treatment for the disease, but Exxon management did not monitor whether or not he abstained from alcohol abuse following in-patient treatment [2]. Furthermore, the National Transportation Safety Board found that Exxon management was not in contact with the hospital that administered treatment before, during, or after the shipmaster was admitted, even though the physician recommended follow-up treatment. Without monitoring the shipmaster's conduct there was no way that management could have verified that the he was not abusing alcohol following his release from the hospital. While the Shipmaster was under the influence the Third Mate had to take control of the ship but was not given the proper 6 hours time off-duty before beginning a 12 hour shift [2]. The allotted time off between shifts is a risk mitigation measure in place to assure that the operator is not a hazard to the ship.

The consequences of Exxon Valdez accident in terms of environmental impact are difficult to estimate, but could certainly be argued as nothing short of catastrophic. The monetary consequence to Exxon was $30 million lost to repair the ship, $2.2 billion for clean-up, and another $1 billion in state and federal settlements. Clearly, the predetermined safety measures regarding ship design, human factors (i.e. proper rest for personnel), and proper safety tools (i.e. on board radar system) were either compromised or neglected by management. The science of system safety seeks to identify these hazards and establish measures to reduce the risk of a mishap, but these measures must be adhered to and verified by management in order to be effective.

When considering human spaceflight, NASA has firsthand experience of the consequences of a mishap due to poor safety management. The importance of system safety is put into perspective when considering the Challenger accident, that ended the lives of seven brave astronauts and cost the county $12 billion [3], or the Columbia accident that took the lives of seven more astronauts and cost the country another $13 billion. The accident investigation boards for both accidents found that deficiencies in system safety were to blame. Following the Challenger accident Ronald Reagan appointed the Roger's Commission to investigate the incident and document the contributing factors. The Commission found four factors that related to deficiencies in system safety, including "a lack of problem reporting requirements, inadequate trend analysis, misrepresentation of criticality, and lack of involvement in critical discussions [4]." The report identified serious flaws in the decision making process, such as the waiving of launch constraints by management without technical oversight or approval. Launch constraints are carefully determined long before the day of launch to ensure that the shuttle is not launched in an unsafe condition. In the case of the Columbia accident, the report found that "the NASA organizational culture had as much to do with the accident as the foam" [2]. Organizational culture, which is determined by top management, will be discussed further in Chapter 5. The simple fact is that both of these accidents could have been prevented with proper attention to system safety principles. While the direct cause of these accidents was technical failure, both accident investigations point out deficiencies in system safety as the underlying causes.

System safety principles can be applied to any technology driven product, or process, comprising complex integrated facets. Generally speaking, management plays a large role in system safety, and the prevention of safety related accidents. The science of system safety provides a structured guideline for managers to follow in order to ensure safe operations, but it does not ensure against deviations from such guidelines. This responsibility lies with management. Management, in this case refers to all levels of management including top management, project management, functional management, and systems engineering management. The accidents mentioned herein are all cases where management failed to adhere to predetermined system safety measures, resulting in the ultimate cost for those who perished, and significant monetary cost to the responsible organizations. Moreover, all of these accidents were preventable with proper attention to system safety practices.

1.1. HISTORICAL PERSPECTIVE ON SYSTEM SAFETY

System safety was introduced after World War II primarily because of public concerns over the safety of nuclear power, aviation, and the chemical industry [6]. Leveson explains how the introduction of technological advancements within the nuclear power, commercial aircraft, and chemical industries were conservative while defense and space industries pushed the envelope with more aggressive introduction of advanced technologies. The Atlas and Titan ballistic missiles are perfect examples of early on technology aggressive programs that did not implement system safety standards, resulting in unforeseen interface problems and low launch success rates [6]. Between the span of

1952 to 1966 the USAF had significant issues with system safety. During this time 7715 aircraft were lost to accidents where 8547 persons perished [7]. It was because of these problems that system engineering and system safety really became accepted as a crucial facet of both the development and operations phases of the product life cycle. "The system safety concept was not the invention of any one person; rather it was a call from the engineering community, contractors and the military to design and build safer systems and equipment by applying a formal proactive approach" [8]. In 1946 Amos L. Wood presented "The Organization of an Aircraft Manufacturer's Air Safety Program," as the first formal mention of system safety principles [8]. In his presentation, Wood describes the need for safety in design, accident investigation, safety education, accident preventative designs, and statistical analysis [8]. This school of thought represents early advancements in system safety and the idea of failure analysis to assess risk. Additionally, Wood is the first to realize that safety must be considered throughout the entire life of the project and not implemented as an afterthought.

"Engineering for Safety," by William I. Stieglitz is another important piece in the history of system safety [8]. Stieglitz was ahead of his time with a call for safety as a specialized discipline and a product design metric. For instance, it wasn't until 2002, when NASA implemented the 2nd Generation Reusable Launch Vehicle program that the agency began to consider safety and reliability as a level 1 requirement [9]. Leveraging the writings of Wood and Stieglitz, system safety really developed through accident investigation and lessons learned. As lessons were learned from early missile tests,

government agencies began to pick up system safety programs. Ericson's review of formal system safety procedures and relevant milestones are shown in Table 1 [8].

Table 1: Formal System Safety Procedures and Relevant Milestones [8]

Year	Milestone
1950	USAF Directorate of Flight Safety Research (DSFR) established at Norton Air Force Base
1955	Navy Safety Center established
1957	Army Safety Center established
1960	Formal system safety organization established at Redstone Arsenal
1960	System safety office established at USAF Ballistic Missile Division
1961	MIL-S-23069 "Safety Requirement, Minimum, Air Launched, Guided Missiles" released
1963	USAF released MIL-S-38130 "Safety Engineering of Systems and Associated Subsystems and Equipment: General Requirements For."
1966	MIL-S-38130 Rev A released
1969	MIL-STD-882 "System Safety Program for Systems and Associated Subsystems and Equipment: Requirements For"

MIL-STD-882 has evolved over the years into a performance-oriented standard that serves as the basis for most system safety programs, in both the military and private sector. The current version of the specification is MIL-STD-882D, "Department of Defense Standard Practice for System Safety" [10]. In the document the standard is described as a tool to manage the risk of environmental, safety, and health mishaps.

At the same time system safety principles were evolving in the military, the private sector and academia were also beginning to recognize system safety as an engineering discipline. In 1963, the Aerospace System Society was established, and from 1964 to 1965, system safety programs were created at the University of California, and the University of Washington [8]. The first system safety program plan was developed for the Minuteman program by The Boeing Company in December of 1960 [8]. All of

the historical information points to the evolution of MIL-STD-882 as the main carrier of advancements in system safety from its initial release in 1969 to the present version released in January of 2000.

1.2. MODERN SYSTEM SAFETY

System safety experts are noticing that traditional system safety techniques are fast becoming insufficient in their ability to produce safer systems [11]. Current system safety models rely heavily on past experiences. That is, failure data is gathered over the life of a program and statistical models are generated to determine the probability of a failure occurring in the future. This philosophy holds only if the historical data is accurately represents the system being analyzed. With rapid technological advancement the reliability based data that system safety engineers use to predict hazard probability are often not directly applicable. Additionally, most aerospace organizations, such as NASA and Boeing, employ a separate safety group that is in charge of reviewing designs with respect to safety and ensuring safety requirements are met. It will be shown that a paradigm shift in the way organizations treat safety is needed to keep up with the rapidly advancing technologies within the aerospace field. While system safety is an evolving science that is struggling to keep up with industry, seven basic principles of system safety that have remained constant [7]:

1. System safety is built into the design, and not implemented as an afterthought
2. System safety deals with the entire system and not just it components or subsystems

3. System safety looks beyond failure based hazards and attempts to identify all hazards inherent in the system
4. System safety relies on analysis rather than experience and standards
5. System safety uses a qualitative approach
6. System safety recognizes tradeoffs and conflicts
7. System safety is not just system engineering

Organizations must develop a system safety plan than satisfies these seven principles. Roles of management in the development and execution of the safety plan, and the consideration that must be given with regard to the seven basic principles is analyzed with respect to the following system safety topics:

1. Systems and Systems Engineering
2. Engineering Management Roles in Product Development
3. Hierarchical Structure of Safety Control
4. Organizational Culture

Through analysis of these topics and current system engineering practices within the aerospace industry it will be shown that safety must be considered throughout the project life cycle as a design metric equal in merit to cost, performance, and schedule. In order to achieve this goal, safety requirements must be taken away from a separate safety group and levied on the functional groups to be implemented, not only during operations, but during the design phase as well. Additionally, the tracking of hazards and residual

risk must remain with functional groups where the technical expertise of the group can be utilized to ensure hazards have been properly identified and mitigated.

Chapter 2: Systems and Systems Engineering

This section examines the system safety engineering practices of the National Aeronautics and Space Administration (NASA) as a means to demonstrate how system safety fits within the systems engineering framework. Therefore, the system and system safety engineering models presented in this chapter are taken from the NASA Systems Engineering Handbook [12], and the NASA General Safety Program Requirements document [13]. These models are chosen because of their maturity. "Since the writing of NASA/SP-6105 in 1995, systems engineering at [NASA], within national and international standard bodies, and as a discipline has undergone rapid evolution. Changes include implementing standards in the International Organization for Standardization (ISO) 9000, the use of Carnegie Mellon Software Engineering Institute's Capability Maturity Model Integration (CMMI) to improve development and delivery of products, and the impacts of mission failures [12]." Additionally, through investigation of the Space Shuttle Challenger and Columbia system safety accidents improvements were identified and implemented, resulting in tested and validated system engineering principles for aerospace applications. For these reasons, the NASA systems engineering process is one of the most mature and well documented processes available to the public. The systems engineering (SE) overview is presented to illustrate how the system safety engineering models need to be integrated within the overall SE process to achieve a safe system, which is one that meets the predetermined safety goals of the project. Recall that the first of the seven basic principles of system safety is that system safety is more than

just systems engineering. Engineering managers must be able to track safety throughout product development, deployment, and operation. This is achieved by treating system safety as an integrated engineering discipline within the SE model. This section includes the definition of a system and examines the NASA system engineering framework. The NASA system engineering framework is broken down into the three major processes of system design, product realization, and technical management. System safety is a technical discipline within the technical management umbrella, but it will become apparent that all aspects of the systems engineering process are connected in one way or another.

2.1 Definition of a System

According to the NASA Systems Engineering Handbook, a system is "a construct or collection of different elements that together produce results not obtainable by the elements alone…elements or parts can include people, hardware, software, facilities, policies, and documents [12]." Breaking down the NASA definition can give further insight into what a system actually is. The first element is people, representing all of the stakeholders involved in the development, manufacturing, testing, operation, and maintenance of the system. Generally speaking, they are managers, engineers, technicians, operators, and customers of the product, and together they design, fabricate, operate, and manage the tasks required for the remaining elements of the system.

A system can be something as large as the Space Transportation System (STS) or as small as an actuating valve in the STS Main Propulsion System (MPS). In most

instances, a system is actually a collection of smaller systems, as is the case with the STS. Figure 1 shows a highly simplified hierarchical view of the STS. The top level STS consists of the External Tank, Orbiter, and Solid Rocket Boosters. Figure 1 shows the sub-system hierarchy for the Orbiter, but the External Tank and Solid Rocket Boosters are also broken down into sets of sub-systems. Separating a product into smaller sub-systems is how system engineers manage complex systems. Each one of the sub-systems can be comprised of one or all of the elements listed in the NASA definition of a system. In the case of the STS, the sub-systems and their elements are combined to launch 50,000 lbs of payload into low earth orbit, a feat that certainly could not be achieved by the sub-systems or elements individually. This illustrates the first part of the system definition; a collection of elements working together to achieve more than possible on an individual basis. In the end, this is the true benefit of a system, but it requires an entire engineering discipline to manage, known as systems engineering.

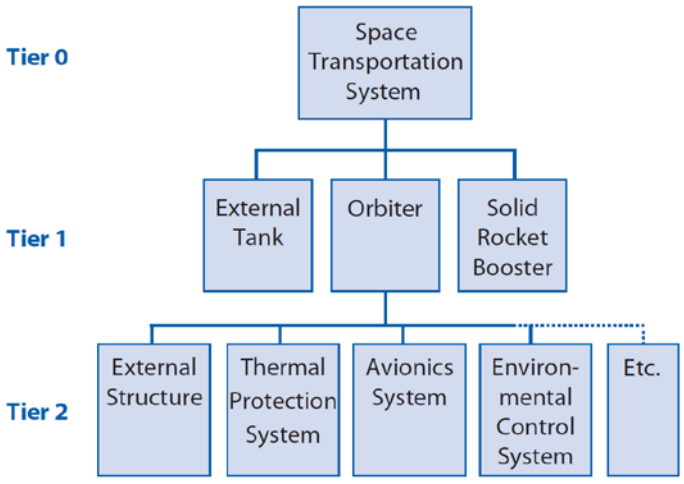

Figure 1: STS Simplified System Hierarchy [12]

2.2 DEFINITION OF SYSTEMS ENGINEERING (SE)

The definition of SE in the NASA Systems Engineering Handbook is "…a methodical, disciplined approach for the design, realization, technical management, operations, and retirement of a system." Due to the complexity of modern systems it is becoming almost universally accepted that a systems approach is necessary for a successful project [14]. Eisner identifies seven key features of a systems approach:

1. Follow a systematic and repeatable process
2. Emphasize interoperability and harmonious system operations
3. Provide a cost-effective solution to the customer's problem
4. Assure the consideration of alternatives
5. Use iterations as a means of refinement and convergence
6. Satisfy all user and customer requirements
7. Create a robust system

This paper will examine the SE engine defined by NASA to demonstrate how these seven principles are applied with a comprehensive SE approach. The NASA SE engine framework consists of three technical processes: system design, product realization, and technical management. The NASA SE engine is shown in Figure 2 [12].

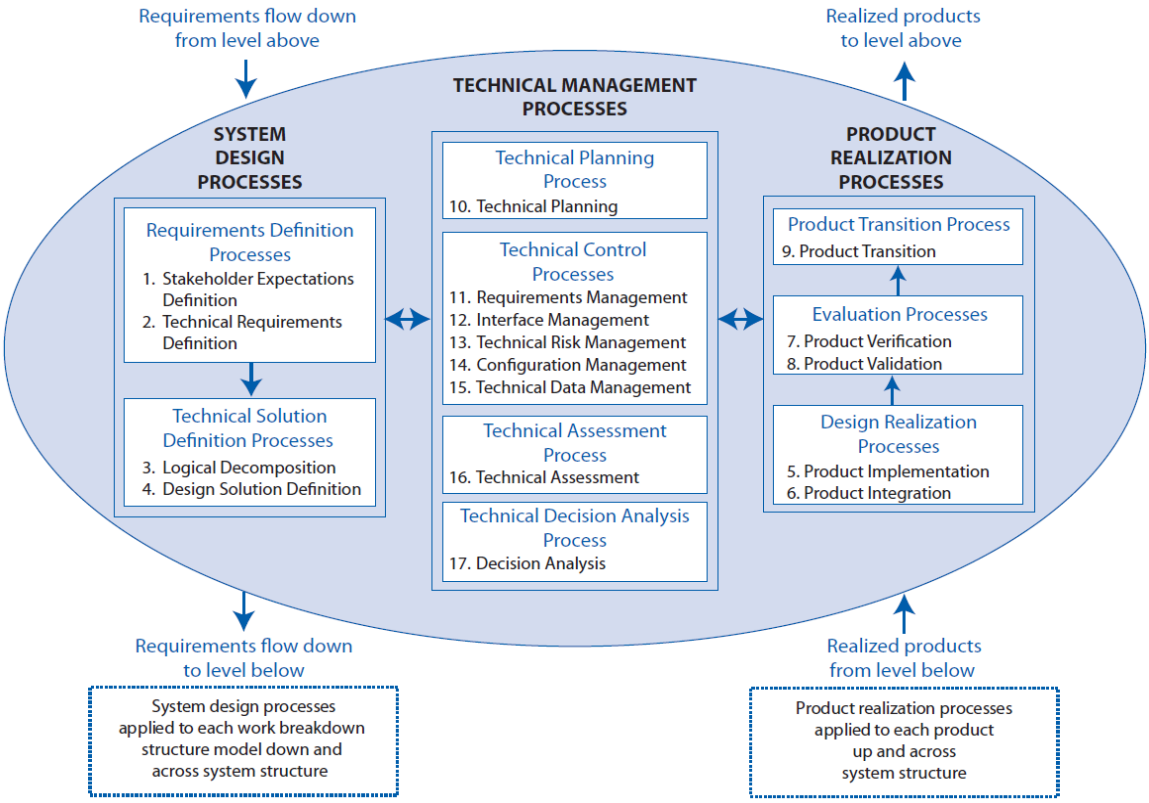

Figure 2: NASA Systems Engineering Engine [12]

The SE process is meant to be iterative and recursive, and applied at each phase of the product life-cycle. NASA defines "iterative" as the "application of a process to the same product or set of products to correct a discovered discrepancy or other variation from requirements," and "recursive" as "the repeated application of processes to design next lower layer system products or to realize next upper layer end products within the system structure [13]." Another common model of the systems engineering engine is the V-model. Shown in Figure 3, the V-model demonstrates the top-down approach in the system design process, the bottom-up approach in the product realization process, and the

technical management taking place between the two. System safety can be thought of as a systems engineering specialty, such as reliability and maintainability, which takes place during the entire system engineering process and throughout the life cycle of the program. Both of these models demonstrate the first of the seven principles of a systems engineering approach, and that is a systematic and repeatable process.

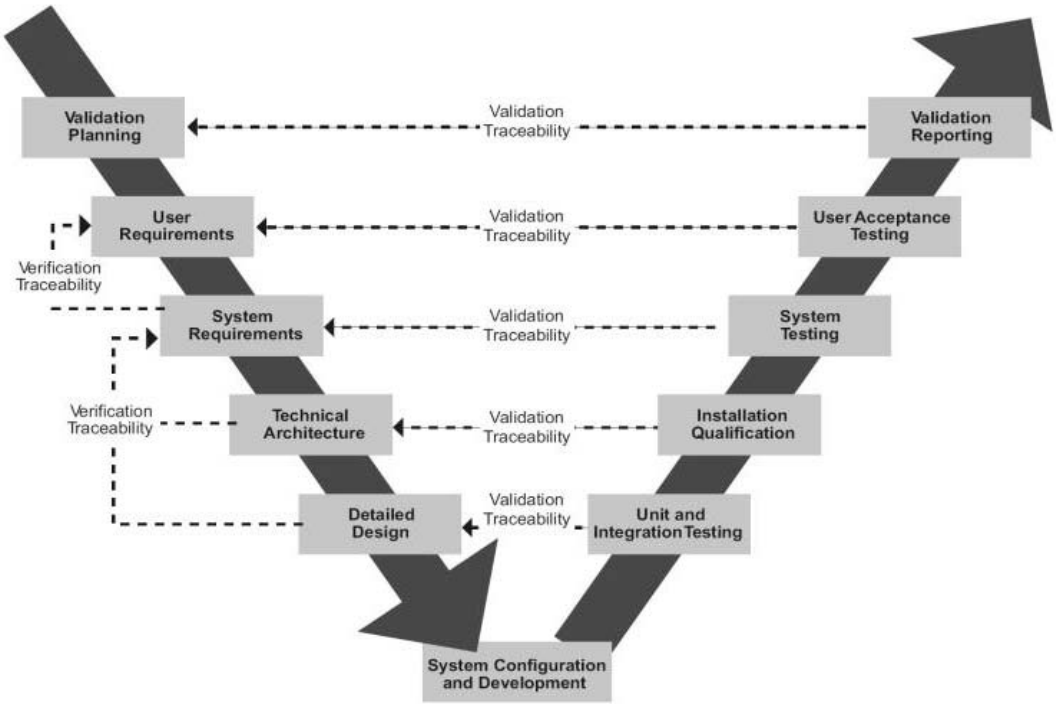

Figure 3: The System Engineering V-Model [15]

The systems engineering V-model can be related to the product life cycle and the different safety analyses that take place during each phase. The life cycle of any project has five major phases: conceptual design, development and test, production, operation, and disposal [16]. The NASA SE engine consists of 17 processes, which are broken

down into three categories: system design, product realization, and technical management.

2.2.1 System Design Processes

The system design process is divided into the two categories of requirements definition and technical solution definition. This process calls for requirements from the top level of the system to flow down through the lower level sub-systems. This takes place until the lowest products in the system are at a manageable state and can be purchased, fabricated, or reused. During the system design process, a concept for the system materializes based on this flow of requirements from the top down. Important product information is obtained from all of the stakeholders. Generally, this information includes concepts of operations (CONOPS), intended uses, and anticipated product life cycle. With this information technical requirements are established in the form of quantifiable, measureable, and succinct baseline technical requirements. Examples of the types of requirements developed during this process are functional, performance, interface, environmental, reliability, and safety. Once established, these requirements are organized hierarchically from the top level down, with the top levels being the customer requirements and the bottom levels representing the implementing organization requirements. Top-level requirements are decomposed as far down as necessary in order to obtain basic system architecture and end product requirements. Finally, alternative design solutions are defined and a trade study of the proposed designs leads to the selection of a final solution. The chosen alternative is developed into a final design

solution ready for production, and system specifications are generated. Using the customer's requirements to develop alternative solutions during the system design process provides a means to converge on the most cost-effective solution that meets the customer's needs.

2.2.2 Product Realization Processes

Since the SE engine is applied during all phases of the product life cycle, the product realization process could refer to the realization of paper studies, hardware, software, models, or the whole system. This process is different than the system design process in that product realization is passed from the lowest level up. The solution formulated during the system design phase is verified against the technical requirements at each level up the system tree, and finally validated against the CONOPS and other stakeholder needs. Generally speaking, verification testing is meant to show that all of the approved requirements are met, while validation testing is meant to prove that the system can achieve the mission objectives described in the CONOPS. The methods of tying requirements to system verification and validation are defined in the Technical Management process, discussed later. The product realization process consists of three separate categories: design realization, evaluation, and product transition. The product realization process framework is shown in Figure 4. The framework clearly shows the three step process of design realization, evaluation, and product transition.

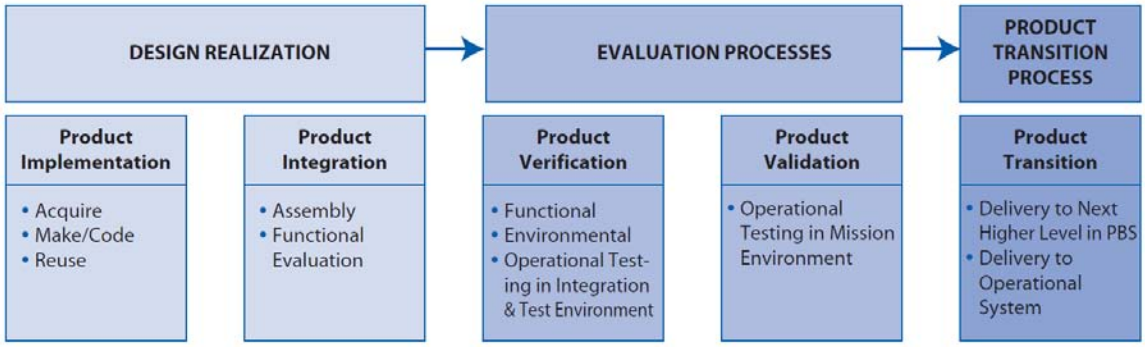

Figure 4: Product Realization Process [12]

At each level, "product" could refer to individual components, lower level sub-systems, or the full up system, depending on how the system hierarchy is defined, and at what point in the overall system the SE engine is being applied. The Product Breakdown Structure (PBS) defines how the system is separated for implementation into the SE engine. The iterative and recursive nature of SE process will eventually result in the integration of the top level system architecture. During the product integration stage, the system engineer must define interfaces and interface characteristics, ensure compatibility across interfaces, integrate lower level products into upper level systems, and document interface characteristics. These tasks culminate in an integrated product ready to be verified, validated, and transitioned to the next level or to the end-user. The product realization process ensures that a robust system is designed by using iterations as a means of refinement and convergence.

2.2.3 Technical Management Processes

The technical management process is comprised of four categories: technical planning, technical control, technical assessment, and technical decision analysis. This takes place during the entire systems engineering process and throughout the life cycle of the product. The technical management of the system serves as a means to connect the product requirements from system design process to product verification and validation from the product realization process. Bridging the stakeholder and the derived technical requirements with product realization ensures that the system will, not only meet requirements, but perform as intended. Without the technical management process, the project's objectives cannot be met. There are eight major tasks in the technical management process: technical planning, requirements management, interface management, technical risk management, configuration management, technical data management, technical assessment, and decision analysis, as shown in Figure 2. These processes take place during one or all phases of the product life-cycle. The technical management process is the "glue" that holds the project together. It provides the CSE a means of emphasizing interoperability and harmonious system operations. Without the technical management process none of the seven key principles of a systems approach could be realized.

2.3 Systems Engineering and System Safety

System safety is a subset of the Technical Management process, but it exhibits many of the same attributes of the system engineering process. First, the system design

process seeks to identify stakeholder needs and requirements in order to develop alternative designs. During this time system safety objectives are defined along with high level requirements with respect to safety. A system safety plan is generated that encompasses the program safety goals, and serves as the basis for safety assessment throughout the development process. In essence, the desired behavior of the system with respect to safety is defined by the safety plan. As the design matures through the system design process, possible hazards are identified and safety controls are established to mitigate the risk of a mishap. There are many types of controls that exist to mitigate risk. Design constraints, such as redundancy in critical components, can be built into the system to inhibit a hazard. Engineers could also implement special processes to protect against a hazard. An example of a risk mitigating process control is the maneuver that Third Mate on the Exxon Valdez was instructed to take in order to safely pass Bligh Reef. When considering process controls, human interaction or automation could be used, both of which pose unique safety related hazards that system safety engineers must consider when assessing risk. Management can also impart controls through organizational structure, company policy, and organizational culture. In addition to management controls, there are outside controls such as government regulations and individual self-interest. Management must be cognizant of these controls in order to ensure safety engineers are addressing all possible hazards, and outside influence from management is not adversely affecting the overall safety of the system.

Chapter 3: Engineering Management Roles in Product Development

It has been established that complex systems require a systems engineering approach to product development. However, proper management of the system's approach and project schedule, cost, and performance require active participation from all levels of management. The most common problems that projects face can be derived from one or more levels of management failing to meet their responsibilities. Whether it is poor planning, loosely defined requirements, inadequate technical skills, or a lack of corporate support, problems in product development originate at the top and, if not mitigated, can cause any project to fail to meet its predetermined goals. Examining the responsibilities of management will later help to identify how system safety principles can be integrated into the processes and culture of an engineering firm. The four levels of management discussed are project management, system engineering management, functional management, and corporate management.

3.1 PROJECT MANAGEMENT

The project manager (PM) is responsible for the overall project schedule, cost, and performance. Project management is broken down into five process groups: initiating, planning, executing, monitoring and controlling, and closing [17]. The PM initiates the project by developing a project charter and identifying all of the project stakeholders. The planning stage is where requirements are collected and project scope is defined. The requirements and scope of the project are close coupled with the initial stages of the system engineering engine where customer needs are analyzed and top level

requirements are generated. The PM needs this information to develop project schedule, define responsibilities, allocate resources, and estimate project cost. Project execution takes place concurrently with the system engineering process. The PM tracks project performance, schedule, and cost during the monitoring and controlling process, and reallocates resources as necessary to keep the project on track. Finally, the PM closes out the project by finalizing all activities. This paper is not intended to be a project management tool, but rather a means of identifying the responsibilities of the project manager with respect to system safety. Chapter 4 will cover the correlations between project management and system safety. In order to achieve this correlation it is necessary to identify some of the common problems in project management. Problems are perceived in terms of three factors: schedule, cost, and performance, known as the "big three" of project and systems engineering management [14]. Eisner identifies seven common reasons why projects encounter problems: articulation of requirements, poor planning, inadequate technical skills, lack of teamwork, poor communication, insufficient monitoring of progress, and inferior corporate support. These common problems can be translated to common problems in managing system safety, as well. Again, this idea will be explored further in Chapter 4.

3.2 SYSTEMS ENGINEERING MANAGEMENT

The number one responsibility of systems engineering management is to identify and develop a solution that meets the customer's expectations. This responsibility usually lies with the Chief Systems Engineer (CSE). The CSE must establish a technical

approach, evaluate alternative designs, develop the preferred system architecture, implement a repeatable systems engineering process, manage the use of computer tools and aids, and serve as technical coach and team leader [14]. The CSE is the technical face of the project that attempts to create a suitable solution to the customer's needs within the constraints prescribed by the project engineer.

3.3 FUNCTIONAL MANAGEMENT\

The roles and responsibilities of the functional manager are dependent upon the organizational structure of the firm. In a typical functional organizational structure, functional managers are responsible for management of resources in the various functions that the organization is divided into. These functions could be engineering, manufacturing, marketing, etc. The functional managers must continually prioritize projects and place resources where they are required the most. This often makes it difficult for project managers to guarantee that the proper level of technical support is provided for their project. Maintaining adequate technical skills and continuity of resource assignments is the main focus the functional manager. This requires effective communication with project management to determine project goals, and corporate management to determine project priority.

3.4 CORPORATE MANAGEMENT

Functional managers, systems engineers, and project managers are all fulfilling the tasks necessary to meet the business goals defined by corporate management. Corporate management defines the course that the company is going to take in order to be

a viable business. When it comes to projects, corporate management sets the organizational culture of the firm by taking relevant government and industry standards, regulations, and laws and developing company standards, policies, and resources. It will be shown in Chapter 5 that organizational culture has a large affect on the success of system safety goals.

Chapter 4: System Safety Overview

System safety is a systematic scientific approach that engineers use to characterize the risk of potential hazards. Most traditional approaches to systems safety involve the identification and management of hazards and their associated risks by leveraging reliability data obtained during product development. However, recent advancements in the field suggest that system safety needs to be an integral part of the system engineering process as a design metric that addresses personnel, equipment, and environmental safety [13]. Recall, the third of the seven basic principles of system safety is to look beyond failure based hazards and identify all hazards inherent in the system. This overview will detail the system safety process and identify the roles and responsibilities of management throughout.

Before delving into the system safety process, it is necessary to define a few key concepts. First, a hazard is defined as a "condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event" [18]. Hazards represent the conditions by which a mishap can take place. A mishap is "an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment" [10]. The NASA system safety requirements, as with most government and commercial methods, leverage MIL-STD-882 for a generalized system approach to hazard analysis. It is the hazard-mishap relationship that constitutes the first major concept of system safety. The second major concept is risk. Risk encompasses to the severity, probability, and impact of a mishap. Together, hazard

analysis and risk assessment drive the system safety process. System safety science will identify and classify the risk of hazards, it is up to management to determine the acceptable level of risk to the program.

4.1 THE SYSTEM SAFETY PROCESS

The core system safety process outlined in MIL-STD-882 consists of eight steps, shown in Figure 5. Further examination of the eight steps reveals that system safety hinges upon hazard analysis and the characterization of risk. Management plays a role in all eight steps of the system safety process. Initially, it is up to the program manager and CSE to develop a system safety plan that addresses resource allocation and defines responsibilities. The PM and CSE must consider the organizational structure of the company when determining these responsibilities. The first item of the seven basic principles of system safety, listed in section 1.3, specifies that system safety must be built into the design, and not implemented as an afterthought. This implies that the program manager must consider system safety from the beginning and attempt to create a comprehensive plan that dedicates resources and defines the safety culture within the project. Organizational culture within the project is something that was found to be one of the major causes of the Space Shuttle Challenger and Columbia accidents, and will be discussed further in Chapter 5.

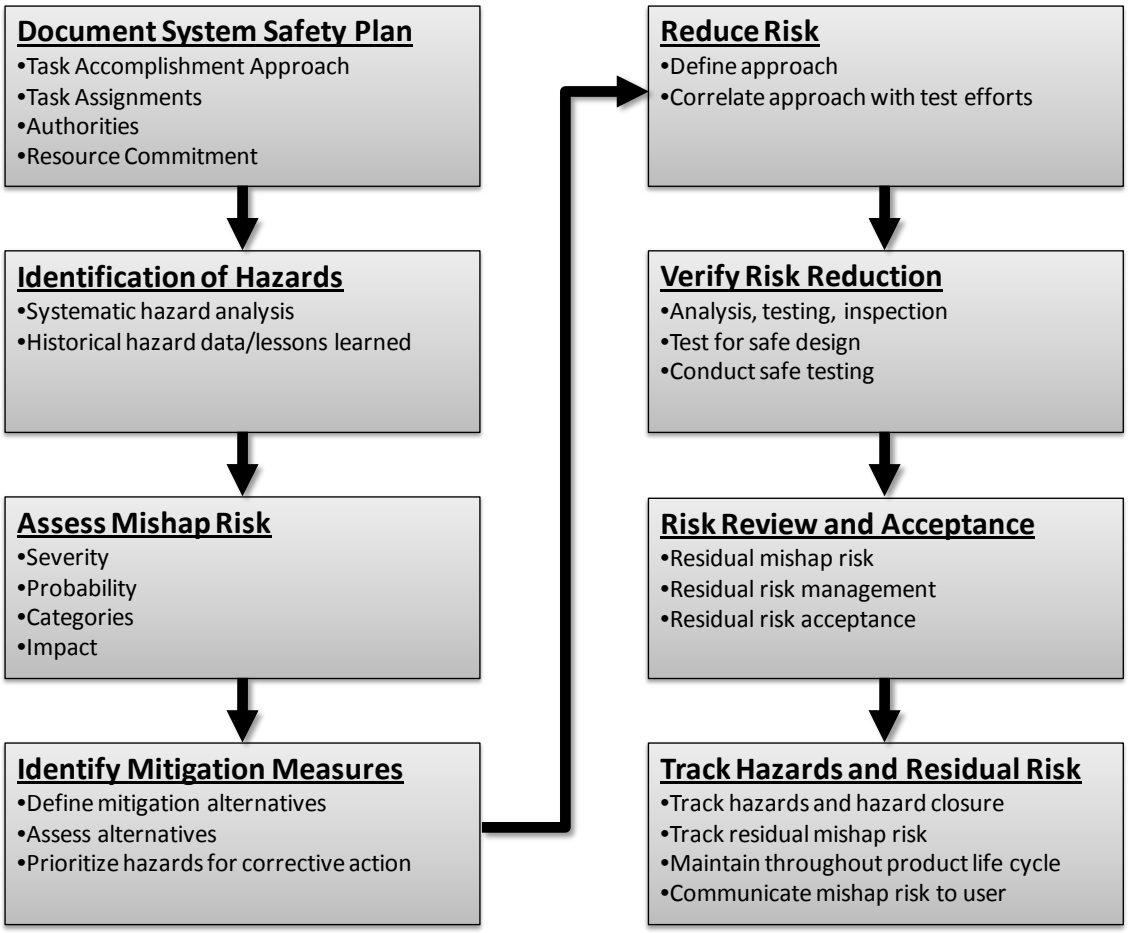

Figure 5: System Safety Process as Defined in MIL-STD-882 [10]

The safety plan lays the groundwork for all the safety related tasks of the project. It specifies the hazard analysis tools that are to be implemented. The following steps, identification of hazards, mishap risk, hazard mitigation, risk reduction, and risk verification, are generally the responsibility of the CSE. However, constant communication between the CSE and the PM throughout these steps is required so that the PM can make informed decisions regarding the allocation of resources and acceptance of unavoidable, or unmitigated, risk.

Identification of hazards is the second step in the system safety process. This constitutes a systematic approach to hazard analysis and a comprehensive assessment of lessons learned on previous projects. Often times the system safety engineers will overlook the lessons learned on previous programs, and sometimes even neglect to learn from mistakes within the same program. This was the case with the Shuttle accidents. Although technical malfunctions that lead to both accidents were noted ahead of time, they were deemed acceptable, and decision makers did not listen to experienced engineers nor did they acknowledge or address the unresolved problems [3]. The CSE must encourage safety engineers to learn from past experiences when attempting to identify all possible hazards. During hazard identification the CSE must remember that hazards do not just exist at the component level. The analysis must extend to the entire system, the second of the seven basic principles of system safety.

The third step in the system safety process is the assessment of mishap risk. Risk is the premise behind the decisions that program management makes regarding safety related issues. The assessment considers risk severity, probability, and impact. NASA describes risk as a function of "triplets," referring to an accident scenario, frequency of occurrence, and consequence [13]. Accident scenarios define the circumstances by which an accident might occur, while frequency is a characterization of the probability of an accident scenario occurring, and the consequence is the severity of the outcome. The categorization of risk usually involves placing all the mishap risk scenarios on a risk matrix to determine whether or not the risk is too high or acceptable. The likelihood and consequence classifications are pre-determined and the level of acceptable risk is decided

during the planning stages. Figure 6 shows the risk process card used by the International Space Station program management. The vertical axis of the risk matrix is the likelihood while the horizontal axis is the consequence. The metrics that define likelihood and consequence are clearly stated on the process card for easy reference. The accident scenarios are categorized and placed on the risk matrix for evaluation. There are thousands of accident scenarios for something as complicated as the space station, so categorization of mishaps is absolutely necessary. It is also crucial that program management determine early in the program what level of risk is unacceptable. Notice the risk matrix on the process card in Figure 6 has three colors. Green represents low risk, yellow represents moderate risk, and red represents high risk. Usually, there are some levels of risk that are unacceptable no matter what the impact to the program.

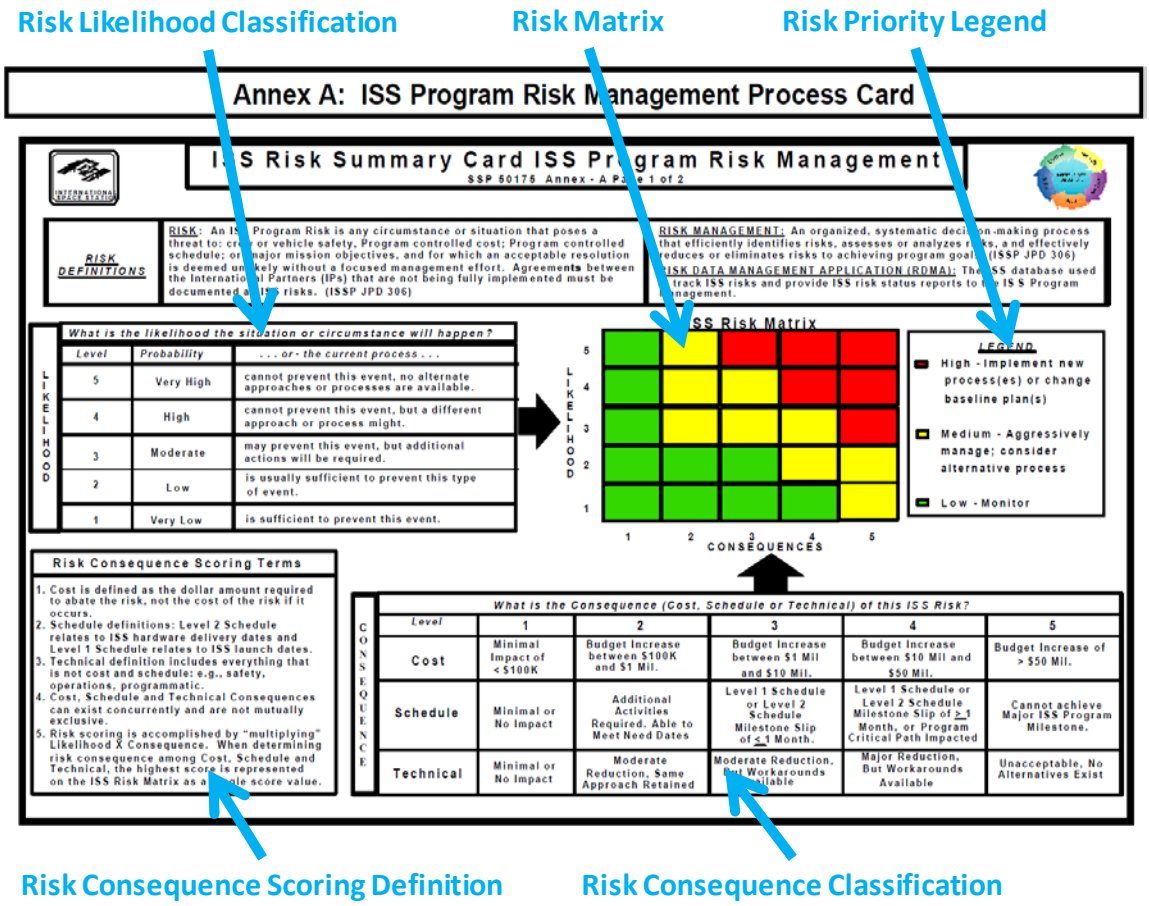

Figure 6: International Space Station Risk Management Process Card [19]

If an accident scenario is deemed acceptable, meaning the likelihood and consequence put the risk too high with respect to established safety goals, then mitigation measures are taken. Identifying mitigation measures is the forth step of the system safety process and establishing the risk reduction approach is the fifth step. It is up to the CSE to determine the risk classification of each hazard and identify mitigation measures to reduce the risk as necessary. All programs are constrained by cost, schedule, and

performance, so mitigation of all risk is typically not possible. Risk that cannot be mitigated must be accepted by the PM. The CSE identifies ways to reduce the risk of all credible accident scenarios, and presents those options to the PM along with the anticipated impact to cost, schedule, and performance. The PM can then prioritize the scenarios based on all metrics and direct the CSE to reduce the risk of those scenarios that represent the highest risk with respect to the program goals. Ways of reducing or mitigating risk include analysis, inspection, or testing. Typically, inspection is the least expensive approach, while testing is the most expensive, and analysis is somewhere in between. Design engineers propose which method is best to reduce risk, while system safety engineers scrutinize the proposed methods. The CSE and PM must allow system safety engineers to evaluate the risk reduction methods; otherwise they could be accepting a plan that cannot deliver on what is promised. This means that the PM must allocate the necessary resources for safety engineers to evaluate the plan, and the CSE must provide the safety engineers with the latitude to do their work. Often times the facts that safety engineers provide can be uncomfortable to the PM and CSE as the safety related issues identified lead to cost and schedule constraints. However, rather than accept the risk reduction plan at face value, the system safety engineer's evaluation provides management with the piece-of-mind that the plan will work. Once the risk reduction approach is established, the PM and CSE must work together to correlate the risk reduction approach with the planned testing of the system. Planned testing of components, subsystems, or the full system, establishes the risk reduction verification criteria, and leads into the sixth step of the system safety process.

The sixth step of the system safety process is verification of risk reduction. By this point all possible hazards have been identified, categorized, prioritized, and assessed. The risk of each hazard has been established and a plan has been created to mitigate high priority risks. Verification is the process of showing that the controlling factors and mitigation rationale support the updated risk classification. Hazard analysis, as with system engineering, implements a closed loop system approach. Figure 7 shows the hazard control process, adopted from the NASA system safety requirements [13]. The sixth step ensures that the plan to mitigate, or reduce, the unacceptable risk is conducted. The risk reduction plan could include analysis, inspection, or testing. Once the plan has been implemented, the risk classifications of the identified hazards are updated. The Hazard Control Process illustrates the hazard-mishap relationship and the controls established to mitigate the mishap risk. Controls could are the measures in place to reduce the likelihood of occurrence, or the measures in place to reduce the severity of occurrence.

The next step is for management to review the updated risk, and either accept the residual risk and move forward, or return back to step four and attempt to further reduce unacceptable risk. Once this iterative process is completed the residual risk is documented in a hazard report for tracking and monitoring purposes. A hazard report contains the residual risk of hazards that could not be controlled or mitigated. Elements of the report are the hazard description, cause, effect, risk, controlling factors, mitigation, and verification. Notice, these elements stem from the tasks outlined in the system safety process. The description is the generic hazard, such as a fire or explosion. The causes

are the events or conditions that may result in a mishap, while the effects are the potential results of each cause. The severity and likelihood of occurrence represent the risk associated with each cause. Acceptable risk is established at the program level during the initial stages of the product life cycle. The controlling factors and mitigations are the measures put into place that prevent the hazard from occurring, such as a fire repression system to control a fire hazard. The hazard report documents the hazard control process shown in Figure 7.

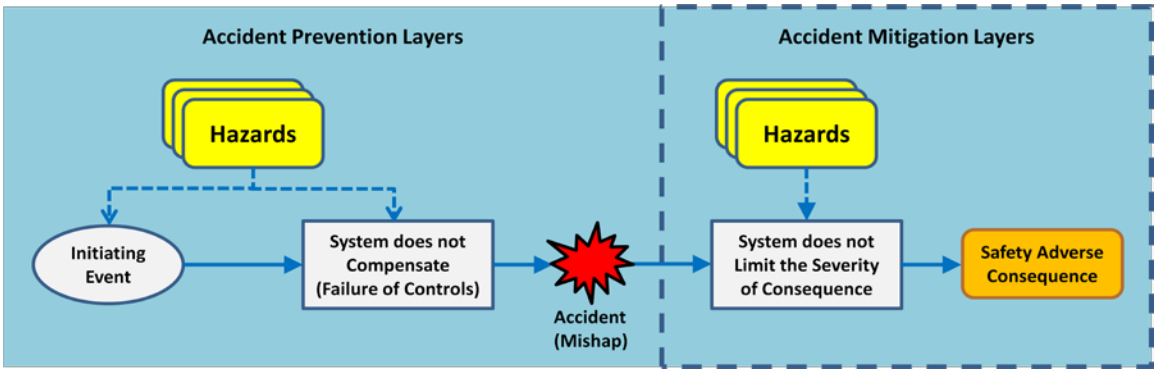

Figure 7: Hazard Control Process as Defined in NASA NPR 8715.3 [13]

Not all hazards are contained within the hazard report. Rather, the hazards that do not meet predetermined risk requirements of the program are those that are controlled by the hazard report. For instance, on the STS program, NASA followed a model of "Fail Operational, Fail Safe (FO/FS) [20]." In other words, the system was designed such that a single failure results in an operational vehicle that can still meet mission objectives, while a second failure results in a safe vehicle that can return the vehicle, crew, and payload home safely. When the risk of a hazard condition did not meet the FO/FS

requirement, it was organized into the hazard report. While the risk rationale for STS is FO/FS, the same system safety tools and principles apply for any organization, regardless of the predetermined risk requirements. The PM must ensure that the project is following the predetermined safety protocols. One of the underlying causes of the Challenger accident was the apparent disconnect between management and engineering. Program management was under intense schedule pressure and had been isolated from the lower levels, and therefore was not properly informed of the booster o-ring hazard [21].

The final step in the system safety procedure is to track hazards and residual risk. The hazard reports represent the primary tool for accomplishing this task. The tracking of hazards and risk are mostly conducted throughout the operations phase of the project. As reliability and safety data is collected on system performance, the hazard analysis and risk assessments are updated. Additionally, design changes during system operation are inevitable, and the CSE must be diligent in ensuring that the system safety process is conducted when those changes are made.

An example of how a design change can affect system safety is the liquid hydrogen drain assist purge, activated late in the launch countdown, for the STS Main Propulsion System. The drain assist purge is a gaseous helium purge that vacates liquid hydrogen propellant from the fill line just prior to launch initiation. When the STS was initially fielded the helium purge was not in place, but added later during the operations phase of the system life cycle. The purge entry point is adjacent to the orbiter on the facility side of the orbiter outboard fill and drain line isolation valve (PV11). The inboard fill and drain isolation valve (PV12) is closed during this operation, as well as the

orbiter replenish valve, but PV11 is open. This essentially opens a path for the helium gas to enter into the orbiter fill and drain line, an 11 foot long 8 inch diameter pipe on the orbiter. The purge starts at approximately T-98 seconds in the count sequence and lasts for 90 seconds. PV11 closes 50 seconds into the purge, isolating any gas that was present in the orbiter fill and drain line. PV12 is adjacent to the main feed line for the SSME during ascent, and it has a relief valve that will relieve gas into the main feed line if the pressure in the line goes above a certain pressure. This is the nominal operation of the valve to prevent the over pressurization of the fill line. When the purge was added, the hazard analysis did not identify the fact that the gas in the fill line could be helium, which if relieved into the SSME feed line could result in cavitation of the high pressure turbo pump and catastrophic failure. The STS went through several launches without addressing this potential hazard. This is just one example illustrating the need for the CSE to be diligent in updating hazards continually throughout the product life cycle. Additionally, program management must provide the CSE with the resources to continually update the hazard analysis.

4.2 Looking Beyond Failure Based Hazards

During various phases of the product life cycle different hazard analysis techniques are implemented and the tools to characterize the hazards in each phase also differ. However, the basic premise behind the system safety process is still based on failure scenarios and supported with reliability data. However, complex systems can pose hazards that are not just failure based.

With most system safety programs, accident scenarios are defined through failure analysis. That is, analysis is conducted based on reliability data that identifies the probability of a component, or sub-system, failure. In his book, *Hazard Analysis Techniques for System Safety* [16], Ericson describes seven different hazard analysis processes that must take place during the various phases of product development and operation to ensure that all hazards are identified, and not just failure based scenarios. The seven hazard analysis types are:

1. Conceptual design hazard analysis
2. Preliminary design hazard analysis
3. Detailed design hazard analysis
4. System design hazard analysis
5. Operations design hazard analysis
6. Health design hazard analysis
7. Requirements design hazard analysis

The hazard analysis types can be thought of as filters that gradually mitigate, or establish controls for, all hazards that could be encountered throughout the product life cycle. Recall, controls are the measures in place that verify the risk classification of the hazard. The hazards that are not controlled or mitigated represent the residual risk to the program and are usually compiled into hazard reports that are monitored and updated throughout the operations phase of the program. There are many tools available to

conduct these hazard analyses, but they all can be classified into two basic techniques—inductive and deductive.

The system safety process uses various inductive and deductive techniques, that complement one another, to make certain all safety Performance Measures (PM) are achieved. Some of the tools commonly used, which can generally be categorized as failure based analysis techniques, are Fault Tree Analysis, Failure Modes Effects Analysis (FMEA), and Critical Items Lists (CIL). FTA is a deductive approach where "conclusions are drawn from a set of premises and contains no more information than the premises taken collectively." [16]. For instance, on the STS there is a hazard scenario where contaminates in the fuel could result in shutdown or catastrophic failure of the main engines. FTA seeks to identify the premises that would allow contaminates to enter into the fuel supply, such as a leaking valve that allows a foreign gas to enter the fuel feed line. The deductive reasoning is: the main engine could explode because of fuel pump cavitation; the fuel pump could cavitate if helium gas enters the fuel supply; and helium gas could enter the fuel supply through a leaking valve. FTA is considered a top-down approach, as shown in this example. FMEA is a bottom-up approach and an example of an inductive hazard analysis technique, where "a conclusion is proposed that contains more information than the observation or experience on which it is based [16]." FMEA is a reliability tool used during design to identify what components can fail, how they can fail, how often, and with what consequences. This information is in turn used to assess the overall reliability of the system. Through inductive and deductive analysis techniques designers seek to identify all possible hazards and assess the probability of

occurrence. The probability component or sub-system failures can be assessed with life-cycle testing of the component of sub-system. The deficiency with these types of analyses is that they may not adequately identify hazards that are not based on a failure scenario.

An example of a non-failure based hazard is a system hazard. A system hazard is a scenario where the system enters into a hazardous state without a failure. An example of a system failure is the Comair flight 5191 accident [22]. The accident occurred because the aircraft lined up to takeoff from the incorrect run way, while the crew was under the assumption that they were in the correct position for takeoff. Comair 5191 is an example of how inadequately controlled human factors can cause an accident. "Accident models that rely largely on failures, holes, violations, deficiencies, and flows can have a difficult time accommodating accidents that seem to emerge from normal people doing normal work in normal organizations," [23]. Dekker refers to the idea of "normal people doing normal work in normal organizations" as the banality-of-accidents, alluding to the fact that most accidents caused by human factors are not due to sabotage or deviance, but rather a scarcity of resources and pressure from outside forces. Shortly before the accident, Comair had recently been purchased by Delta, and corporate management had demanded wage cuts for the pilots [22]. Nelson states, "Management believed that their corporate strategic actions had nothing to do with safety; that people would, somehow, leave their personal fears and emotions outside the workplace door and remain undistracted while doing their job, even when those distracting fears and emotions

were propagated by management inside the workplace." Management must be aware that outside forces can drive system hazards when human factors are involved.

Chapter 5: Additional System Safety Topics for Engineering Managers

When considering system safety, the ideal goal is to develop and operate systems free of hazards, but this is unachievable given the fact that most complex systems are inherently hazardous [16]. Examples include the STS, commercial aircraft, and nuclear power plants. Additionally, these systems are operated and maintained by humans, considered an integral part of the system, and as such are subject to human error. Development and operation of complex systems is a balance between realized benefits and associated risk. Ericson describes safety as analogous to life in that it is a matter of knowing, identifying, and controlling risk [16]. Systems safety provides safety engineering managers a means of identifying, managing, and mitigating hazard risk. It is up to engineering managers to interpret the system safety data and determine the accepted level of risk for a given project or application.

It is easy to lose sight of safety when constrained by cost and performance goals, but the cost of a safety related mishap could significantly outweigh the costs of a comprehensive and uncompromising safety plan. For instance, an organization with a 5% profit margin would have to have sales of $500,000 to pay for a $25,000 mishap. Safety must be engrained into the organization at all levels and considered as a design metric just like cost and performance. To achieve this goal engineering managers must understand the hierarchical structure of safety control and the effect of organizational culture on system safety.

5.1 Hierarchical Structure of Safety Control

To gain an understanding of how engineering managers can affect system safety, dissection of the safety control hierarchy is necessary. Recall, safety controls are the measures in place that either reduce or mitigate the risk of a mishap. Whereas, the hierarchical structure of safety control represents the flow of constraints from the top levels of the project organizational structure through to the lower levels. It also illustrates the connections between system development and system operations. Figure 8 is the general form of the hierarchical structure of Socio-Technical Control [24]. Socio-technical refers to the social constraints and technical constraints that exist within a project. The system safety process must address both factors. Nancy Leveson, professor of Aeronautics and Astronautics at MIT, has developed this generalized model to illustrate the need for clear communication between levels to achieve a safe system.

The left side of the hierarchical structure shown in Figure 8 represents system development while the right side represents system operations. It can be seen that the structure covers the entire life cycle of the project from inception through manufacturing and into operations. At the top of each side lies Congress and Legislatures because the laws and regulations that governments set will have a profound effect on system design. With the case of NASA, the government dictates the programs that the agency will pursue and allocates funding. On both sides of the hierarchy there is a connection between government legislation and government regulatory agencies. One example of a government regulatory agency is the Federal Aviation Administration that dictates many aircraft design and operational requirements, many of them with regard to safety such as

procedures for aircraft operations. Company management is the next step down the hierarchical chain of requirements. Management sets the safety policies and standards that the project and operations manager's must follow, and allocates resources for the project. This is management's first responsibility with respect to safety in the hierarchy, but it can be seen that project management, manufacturing management, and operations management all have a responsibility of taking applicable laws and regulations in account. What is necessary to maintain a safe system really goes beyond what is required by law, though. It begins with the organizational culture that is present within the firm, and that culture is dictated by management.

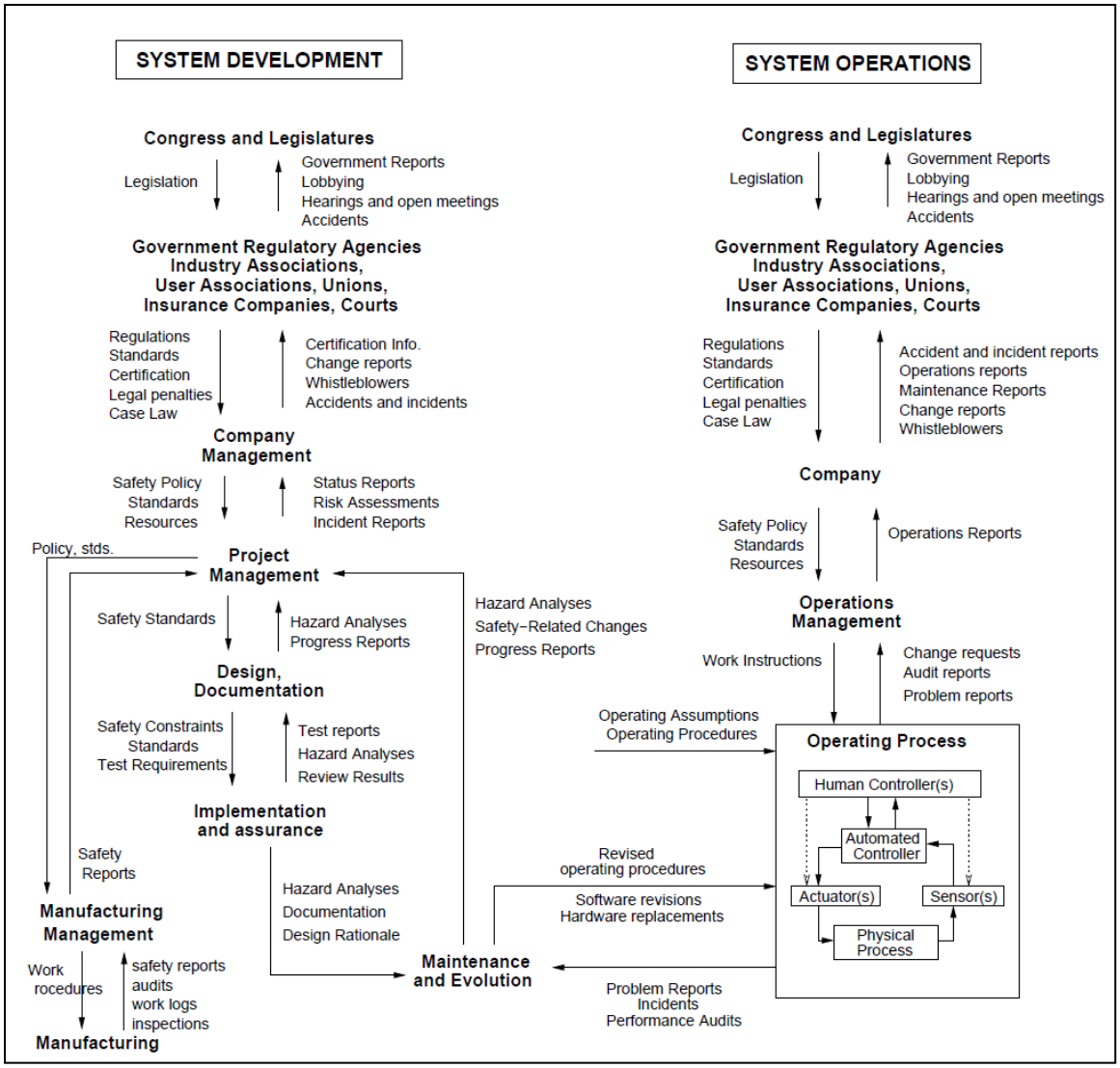

Figure 8: Hierarchical Structure of Socio-Technical Control [24]

5.2 The Influence of Organizational Culture on System Safety

Following the Challenger accident many safety measures were put into place to ensure that outside influences could not drive another launch under unsafe conditions. However, in 1995 a Space Shuttle Management Review Team found that "a myriad of

safety requirements levied on customers…have a significant impact on the design and integration…[5]." Under this premise the team recommended that NASA "restructure and reduce overall safety, reliability, and quality assurance elements" [5]. After experiencing the Columbia accident it is obvious that the team was under a false perception of risk. The question is what drives management to make such decisions when in hindsight they are clearly flawed? One answer is that the evolution of the organizational culture within the company clouds the judgment of management and drives irrational decisions.

In the early days of NASA, the organization was called upon to complete what were thought to be impossible tasks. Because of this NASA had to become a "high-performance government organization" capable to rising to the challenges it faced [25]. For all intents and purposes, NASA was very successful in the early days of space flight with the completion of the Mercury, Gemini, and Apollo programs without losing any astronauts on a space flight mission. However, as with all government organizations, NASA started to become excessively bureaucratic and their employees began to resist new ideas [25]. The obvious troubles with the Space Shuttle are not the only issues NASA has experienced over the past two decades. There was the Orbiting Carbon Observatory satellite that failed to reach orbit due to a problem with the payload fairing in 2009, the Demonstration of Autonomous Rendezvous Technology space craft that collided with the rendezvous satellite in 2005, the Genesis space craft whose parachutes failed to deploy and crashed into the earth in 2004, the Mars Polar Lander that crashed into the surface of Mars in 1999, and the Deep Space 2 penetrator space craft that failed in 1999. According to a study by Howard McCurdy, the decline in NASA can be attributed to the organizational culture of the company. Early on NASA had an adaptive culture that supported high levels of performance [25]. One of the main reasons for this

success was that employees were empowered to make decisions and use their own discretion when faced with technical challenges. As the organizational culture changed the ensuing bureaucracy made it impossible for engineers to have the same flexibility. This inevitably resulted in missed milestones, increased cost, and mission failure on numerous occasions.

Engineering managers must be cognizant of how cultural norms within the company affect the "big three" of project and systems engineering management, schedule, cost, and performance. However, these three measures of a project cannot be looked at independently of safety. Through policy changes and standard company practices management can influence culture to include safety as a driving factor throughout the life-cycle of the project.

Chapter 6: Conclusion

System safety was introduced shortly after World War II due to public concerns over safety in the nuclear power, aviation, and chemical industries. It evolved over the years and eventually took its current form in MIL-STD-882D. Since its inception in 1969, MIL-STD-882 has been the main carrier of advancements in system safety and serves as the basis for most modern system safety plans. The rapid technological advancements in the modern era require management to create and diligently follow a system safety plan that exudes the following basic principles [7]:

1. System safety is built into the design, and not implemented as an afterthought
2. System safety deals with the entire system and not just it components or subsystems
3. System safety looks beyond failure based hazards and attempts to identify all hazards inherent in the system
4. System safety relies on analysis rather than experience and standards
5. System safety uses a qualitative approach
6. System safety recognizes tradeoffs and conflicts
7. System safety is not just system engineering

System safety principles can be applied to any technology driven product, or process, comprising complex integrated facets. It is a systematic scientific approach that engineers use to characterize the risk of potential hazards. Management plays a large role

in system safety, and the prevention of safety related accidents. The science of system safety provides a structured guideline for managers to follow in order to ensure safe operations, but it does not ensure against deviations from such guidelines. This responsibility lies with management. Management, in this case refers to all levels of management including top management, project management, functional management, and systems engineering management.

Engineering managers must be able to track safety throughout product development, deployment, and operation. This is achieved by treating system safety as an integrated engineering discipline within the SE model. However, most organizations have a separate safety group that evaluates proposed designs and identifies areas where safety is an issue. With this approach it is very difficult to build safety into the design and technical teams are often called upon to make design changes late into the program. The result is increased design complexity and, in almost all cases, cost overruns. Additionally, identified hazards and residual risk are not easily tracked and maintained as the program ages. Following the Columbia accident, NASA took control of the STS hazards away from the safety group and placed it into the hands of the technical teams because they realized the hazards were not being maintained properly [3]. It is not feasible to expect the technical teams to integrate safety into the design unless it is considered a design metric just as cost and performance.

The system safety process consists of eight steps with topics including development of a system safety plan, identification of system hazards, risk assessment and management throughout the product life cycle, and tracking of hazards and residual

risk during operations. It is impossible to design systems free of hazards so it is crucial that the entire team understands the safety requirements up front so safety can be built into the design and not treated as an afterthought. Fielding a safe system also depends on management's ability to communicate risk with the technical team, and the proper allocation of resources with respect to system safety. Proper communication of risk requires the CSE and PM to be in tune with lessons learned from previous projects. In order to ensure that the allocation of resources towards safety is sufficient, management must develop a clear and comprehensive safety plan during the planning stage of the project and not after a design exists. The plan must consider hazards not only at the component and sub-system levels but also at the integrated system level. Ideally, the plan should be intertwined with the overall system engineering process so that safety requirements drive design just as cost and performance do. NASA has become aware of this fact as evidenced in the latest version of the NASA General Safety Requirements regarding system safety [13].

References

[1] McCarty, Jennifer and Foecke, Tim. *New Forensic Discoveries What Really Sank The Titanic.* New York: Citadel Press, 2008. Print.

[2] National Transportation Safety Board. "Grounding of U.S. Tankship EXXON VALDEZ on Bligh Reef, Prince William Sound Near Valdez, AK March 24, 1989." NTSB, 1989.

[3] Columbia Accident Investigation Board. "Columbia Accident Investigation Board Report Volume 1." Government Printing Office: Washington D.C., 2003.

[4] Presidential Commission on the Space Shuttle Challenger Accident, *Report of the Presidential Commision*. Washington D.C.: Government Printing Press, 1986.

[5] NASA Technical Memo. "Report of the Space Shuttle Management Independent Review Team." NASA-TM-110579, 1995.

[6] Leveson, Nancy. "An introduction to System Safety." ASK Magazine Summer 2008: pp. 20-23. Print.

[7] Leveson, Nancy. "White Paper on Approaches to Safety Engineering." *Nancy Leveson's Home Page*. Web. Aug. 2010.

[8] Ericson, Clifton. "A Short History of System Safety." Journal of System Safety Vol. 42 No. 3 (2006). Web.

[9] Safie, Fayssal M. and Maggio, Gaspare. "The Quantitative Safety and Reliability Approach For NASA's Second Generation Reusable Launch Vehicles." NASA Astrophysics Data System. Web. 11 June 2002.

[10] MIL-STD-882D. *Department of Defense Standard Practice For System Safety*. Every Spec. Web. 10 Feb 2010.

[11] The System Safety Society. "System Safety: A Science and Technology Primer". The New England Chapter of the System Safety Society. Web. April 2002.

[12] NASA/SP-2007-6105 Rev1. *NASA Systems Engineering Handbook*. National Aeronautics and Space Administration. Washington, D.C. March 2008.

[13] NASA NPR 8715.3. *NASA General Program Safety Requirements Rev C*. National Aeronautics and Space Administration. Washington, D.C. December 2006.

[14] Eisner, Dr. Howard. *Essentials of Project and Systems Engineering Management*. Hoboken, NJ: John Wiley & Sons, Inc., 2005.

[15] Turner, Dr. Richard. "Toward Agile Systems Engineering Processes." Journal of Defense Software Engineering. Web. April 2007.

[16] Ericson, Clifton A. *Hazard Analysis Techniques for System Safety*. Hoboken, NJ: John Wiley & Sons, Inc., 2005

[17] ANSI/PMI 99-001-2008. *A Guide to the Project Management Body of Knowledge*. Newtown Square, PN: Project Management Institute, 2008.

[18] FAA-AIR-m-8040.1. *Airworthiness Directives Manual*. Federal Aviation Administration, 2003.

[19] NASA SSP 50175 Rev A. *International Space Station Program Risk Management Plan.* Houston, TX: Johnson Space Center, 2002.

[20] Kezirian, M.T. "Mission Assurance and Flight Safety of Manned Space Flight: Implications for Future Explorations of Moon and Mars." Houston, TX: The Boeing Company, 2002.

[21] Mahler, Julianne. *Organizational Learning as NASA: The Challenger and Columbia Accidents.* Washington D.C.: Georgetown University Press, 2009.

[22] Nelson, Paul S. "A STAMP Analysis of the LEX Comair 5191 Accident." Sweden: Lund University, June 2008.

[23] Dekker, Sidney W. *Ten Questions About Human Error: A New View of Human Factors and System Safety.* New York: CRC Press, 2005.

[24] Leveson, Nancy. "A New Accident Model for Engineering Safer Systems." Safety Science Vol 42, No. 4. pp. 237-270. April 2004.

[25] McCurdy, Howard E. "Inside NASA High Technology and Organizational Change in the U.S. Space Program." Baltimore, MD: Johns Hopkins University Press, 1993.

[26] "Culture." *Mirriam Webster Online Dictionary*. 2010. Mirriam-Webster Online.

[27] Schein, Edgar H. *Organizational Culture and Leadership, 4th Edition.* Hobeken, NJ: John Wiley & Sons, 2010.

[28] Health and Safety Executive. "Introduction to Human Factors." Great Britain: Health and Safety Executive. Web. 2010.

Vita

After graduating from Embry Riddle Aeronautical University with a Bachelor's degree in Aerospace Engineering, Jerald Adam Webber was employed by NAVAIR in China Lake, CA as a solid rocket motor design engineer. Jerald then moved on to General Atomics Aeronautical Systems where he specialized in system integration on unmanned aircraft. Jerald is currently employed as a propulsion engineer for Boeing Space Exploration in Houston, TX, where he lives with his wife Belinda

Email address: Jerald.A.Webber@gmail.com

This thesis was typed by Jerald Adam Webber.